METHOD FOR AUTHENTICATION OF A STRING OF INPUT CHARACTERS

Background of the Invention

1. Field of the Invention

The invention relates to a method for use in authenticating an input character string.

2. Description of the Prior Art

A method of this type is disclosed in EP-A-0399587. With the known method, the function ("algorithm") applied for enciphering consists of a non-linear function formed by a substitution box ("S box") generated as a function of the key. The '587 European patent application provides no further description of the way in which the substitution box is generated. For obtaining good statistical properties of the output of the substitution box with respect to variable input, a string of characters obtained by applying the substitution box is combined with just as long a string of statistically well-distributed characters. The string of characters obtained in this connection may be used for enciphering a string of input characters to be enciphered into an enciphered string of output characters. By applying a key-dependent substitution box instead of a permanent substitution box, the enciphering function is reinforced.

An objection to the known method is that, when the same key is nearly always used, reinforcement of the enciphering function in practice is appreciably annihilated. Such may occur, e.g., upon authentication when using a chip card, such as a calling card and a GSM card.

Summary of the Invention

The object of the invention is to exclude the drawbacks of the known method.

In accordance with the present invention, the sender of the enciphered string of output characters and the receiver of the series must both dispose of the same key and the string of input characters used for enciphering, at any rate the portion of the latter series used for modifying the function. As a result, the method is particularly suited for authentication, the receiver of an enciphered string of characters being capable of checking whether a sender having an identity suggested to the receiver has utilized a corresponding key, and in the event of a positive outcome of that check, the identity of the sender is ensured to the receiver.

The string of characters used for modifying the function is particularly variable and is, e.g., a challenge number generated per session, any (different) number, or a variable attribute of the sender, such as a balance kept up to date on a chip card.

If the non-linear function used for enciphering were an invertible function, the receiver of the enciphered string of characters may carry out the check using the same function, the same key and the received string of characters as an input for the function. The result must be equal to the string of input characters used for enciphering. Since the receiver may also carry out the check by executing the same operations as the ones carried out by the sender, the series received by the receiver has to be equal to the series generated by the receiver. In such case, it is not required that the function be an invertible function, as a result of which, in the event of the complexity remaining constant, there may be realized a stronger enciphering function which is more resistant against attacks.

The function applied to enciphering preferably is a non-linear function which may be formed by way of a substitution box or a cryptographic function, such as a function in which, depending on the input and the key, specific operations are carried out or not.

It is noted that EP0801477 discloses an encryption method in which an "internal state" is controlling an encryption function which h, in each encryption round, modifies the encryption function. According to the present invention, the encryption function is modified only once, in an initial step, while always, after the initial modification, the same encryption function is used in every new encryption round. Contrary to that, in the known method the encryption function is modified in every encryption round. Further, in the known method the encrypting function is not modified on the basis of the input txt. According to the present invention the input text forms an essential parameter in modifying the encryption function.

Next, it is noted that US4979832 discloses an enciphering method in which a pseudo-random input string is added to an encryption function. The pseudo-random string used in the encryption function also has to be available in the decryption process. In the known method the encryption function is dynamically (continuously) modified, during the encryption processes. This is essential in that method otherwise the system would be highly insecure. According to the present invention, however, there is only an initial modification of the encryption function, prior to the encryption process itself. Consequently, during the subsequent encryption

process the encryption function is not changed any more. The known method is aimed at encryption/decryption. The method according to the invention is specifically designed for authentication and even can in practice not be used for encryption/decryption.

Brief Description of the Drawings

Further properties and advantages of the invention will become clear from the explanation following below of embodiments of the invention in conjunction with the enclosed drawings, in which:

FIG. 1 shows a diagram of a known enciphering function;

FIG. 2 shows a diagram of a first embodiment of the invention;

FIG. 3 shows a flow diagram for the operation of the embodiment according to FIG. 2; and

FIG. 4 shows a second embodiment of the invention.

Detailed Description

By way of a block 1, FIG. 1 presents a known enciphering function (or encryption function). The enciphering function utilizes one or more functions 2, also presented by blocks. Assuming a string of input characters IN on line 3 to be enciphered, the enciphering function using a secret key 4 determines an enciphered string of output characters EXIT on line 5. The known enciphering function DES [= Data Encryption Standard] operates according to said principle, eight non-linear functions being used which are formed by substitution boxes ("S boxes"). The invention is not limited, however, to the DES function; neither is it limited to using non-linear functions and substitution boxes for the functions.

FIG. 2 shows a diagram of an enciphering function (denoted as enciphering algorithm) 7 based on the enciphering function of FIG. 1, but according to the invention. The functions are indicated by reference numeral 8. The functions 8 may be modified by applying associated modification functions (denoted as modification algorithms) 9 based on the string of input characters IN on line 3 or part thereof. The modification functions 9 need not be equal.

Below, the operation of the enciphering function of FIG. 2 will be explained with reference to the flow diagram of FIG. 3.

A modification function 9 modifies the function 8 based on a string of modification characters initially derived from the string of input characters IN (block 11).Modifying the function 8 takes place in several steps, namely, the steps n=0 to n=Nmax inclusive, Nmax being permitted to be permanent or also depending on, e.g., the series IN. That is why, at the start of the modification of the function 8, a step counter is reset (block 12). Subsequently, the function 8 is modified, based on the value

of n and the modification series (block 13). Then the number of steps counted is incremented by 1 (block 14).Subsequently, it is checked whether the function 8 has already been modified the maximum number of times (block 15).When this condition is met, the modification of the function 8 is terminated; otherwise the string of modification characters are modified (step 16) and the function 8 is modified once again based on the new value of n and the modified string of modification characters (step 13).In Box I following below, an example is given for the operation of the enciphering function 7 shown in FIG. 2.

TABLE I

Step n	String of modification characters for n>0 x(2):= (x(0) + x(1))mod8			From step n=0, exchange y(nmod8) and y(x(0))
	x(0)	x(1)	x(2)	i: 0 1 2 3 4 5 6 7 / y(i): 3 0 5 7 6 4 1 2
0	5	2	3	4 0 5 7 6 3 1 2
1	2	3	7	4 5 0 7 6 3 1 2
2	3	7	5	4 5 7 0 6 3 1 2
3	7	5	2	4 5 7 2 6 3 1 0
4	5	2	4	4 5 7 2 3 6 1 0
5	2	4	7	4 5 6 2 3 7 1 0
6	4	7	6	4 5 6 2 1 7 3 0
7	7	6	3	4 5 6 2 1 7 3 0
8	6	3	5	1 5 6 2 4 7 3 0
9	3	5	1	1 2 6 5 4 7 3 0

It is assumed that the set of characters comprises eight characters, shown in the Table with the numerals 0 to 7 inclusive. It is further assumed that the function 8 is formed by a substitution box. This box may be realized by a rewritable memory having eight memory locations containing addresses or sequential numbers 1=0...7. The memory locations each comprise one of the characters, each character figuring only once in the memory locations. In Table I, the content of a memory location having address or sequential number i is indicated by y(i). Initially, the memory locations for i=0...7 contain the characters 3, 0, 5, 7, 6, 4, 1, 2, respectively. This string of characters forms an initial substitution box. A character of a string of characters to be enciphered is considered

to be address or sequential number i, and is replaced by the character in the memory location having that address. According to the initial substitution box of Table I, e.g., 0 is therefore replaced by 3, 1 by 0, 2 by 5, ..., 7 by 2.

Before a string of characters to be enciphered is actually enciphered, according to the invention the initial substitution box is modified first. According to the example of Table I, modification takes place in ten steps (step n=0 to n=Nmax inclusive). The modification takes place depending on the characters of the string of characters to be enciphered, at any rate of several characters thereof. In Table I, the characters to be enciphered which are used for the modification of the substitution box are the characters 5, 2 and 3 indicated at step n=0. These characters are allotted to variables x(0), x(1) and x(2), respectively.

During the first step with n=0, the character y(n), i.e., the character 3 of memory location 0, is exchanged with the character y(x(0)), namely, character 4 of location x(0)=5. In Table I, for clarity's sake, the exchanged characters of the substitution box of eight characters are underlined for each of the ten steps n=0, ...9.

Subsequently, there is calculated an auxiliary variable h, which is equal to:

h=(x(0)+x(1)) modulo (the number of possible characters),
or in the example
h=(x(0)+x(1)) modulo 8.

Subsequently, the characters of the string of modification characters x(0), x(1) and x(2) are replaced as follows (":=" means "becomes", i.e., an allotment).

x(0):=x(1),
x(1):=x(2), and
x(2):=h.

For each step, modifying characters based on the step number and the characters of the string of modification characters are repeated a suitable number of times, in the example of Table I Nmax+1=10 times. At the end of said modification character, the initial substitution box:

3, 0, 5, 7, 6, 4, 1, 2
has been replaced by a final substitution box:
1, 2, 6, 5, 4, 7, 3, 0.

Subsequently, the characters of an input series to be enciphered may, according to the order of the characters in the eventual substitution box, be replaced for providing an output string of enciphered characters.

As a result, in the example the string of input characters 5, 2, 3 are replaced by 7, 6, 5, respectively. Said string of output characters are used for possible further steps of the enciphering character.

FIG. 4 shows the diagram of an enciphering function (also denoted as enciphering algorithm) 18 which differs from the enciphering function 7 of FIG. 2 in that the modification function 9 is replaced by a modification function (denoted as modification algorithm) 19. Just as the modification function 9, the modification function 19 depends on a number of characters IN to be enciphered, but in addition on a number of characters of the key on line 4.

Table II offers an example of the operation of the modification function 19.

TABLE II

Step n	String of modification characters for n>0 x(2):=(x(0) + x(1))mod8 x(0) x(1) x(2) x(3) x(4)	From step n=0, exchange y(nmod8) and y(x(0)) i 0 1 2 3 4 5 6 7 y(i) 3 0 5 7 6 4 1 2
0	5 2 3 2 4	4 0 5 7 6 3 1 2
1	2 3 2 4 7	4 5 0 7 6 3 1 2
2	3 2 4 7 5	4 5 7 0 6 3 1 2
3	2 4 7 5 5	4 5 0 7 6 3 1 2
4	4 7 5 5 6	4 5 0 7 6 3 1 2
5	7 5 5 6 3	4 5 0 7 6 2 1 3
6	5 5 6 3 4	4 5 0 7 6 1 2 3
7	5 6 3 5 2	4 5 0 7 6 3 2 1
8	6 3 5 2 3	2 5 0 7 6 3 4 1
9	3 5 2 3 1	2 7 0 5 6 3 4 1

Table II differs from Table I only in that the string of modification characters x(0), x(1), x(2) are completed by x(3), x(4). The characters x(3) and x(4) are derived from the key 4. In the example of Table II, the initial string of modification characters is 5, 2, 3, 2, 4. According to Table II, the eventual substitution box is:

2, 7, 0, 5, 6, 3, 4, 1.

The string of input characters IN having the characters 5, 2, 3 is replaced, according to said eventual substitution box, by the enciphered string of output characters EXIT on line 20 having the characters 3, 0, 5.

The characters of the initial substitution box may be sorted at random for as long as both the sender of a string of enciphered characters 5 (see FIG. 1) and the receiver of the string of enciphered characters use the same initial substitution box. If it is possible to always meet this condition, the enciphering function may be reinforced by using, as an initial substitution box, a substitution box used during a preceding enciphering process, e.g., the most recently used eventual substitution box. If there is a danger that this condition is not always met, it may be provided that the receiver of the string of enciphered characters 5 recalls several of such preceding substitution boxes and uses an older one thereof if deciphering the series received leads to a negative check result.

Since, both during enciphering a string of characters and during deciphering thereof, the keys used must be equal and knowledge must be available on the string of input enciphered characters, the receiver of the enciphered series may carry out exactly the same operation, i.e., enciphering, as the receiver has carried out, and compare the results to one another. In this event, a non-invertible function may be used for the function which, in the event of constant complexity, makes a stronger enciphering function possible.

The modification functions explained in conjunction with Tables I and II serve only as an example. For modifying the string of modification characters there may be applied, e.g., for each step, more than two and/or a different number of modulo additions, and the characters of the modification series may be rearranged in other ways instead of by way of simple shifting.